(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 107959552 B
(45)授权公告日 2023.08.22

(21)申请号 201711023723.3
(22)申请日 2017.10.27
(65)同一申请的已公布的文献号
申请公布号 CN 107959552 A
(43)申请公布日 2018.04.24
(73)专利权人 浙江浙大网新众合轨道交通工程有限公司
地址 310052 浙江省杭州市滨江区网新双城大厦4幢14楼
专利权人 浙江众合科技股份有限公司
(72)发明人 梅瑜华 师秀霞 刘德勇
(74)专利代理机构 杭州华鼎知识产权代理事务所(普通合伙) 33217
专利代理师 夏华栋
(51)Int.Cl.
*H04L 1/1607*(2023.01)
*H04L 9/08*(2006.01)
*H04L 9/32*(2006.01)

(56)对比文件
CN 103297563 A,2013.09.11
CN 106789259 A,2017.05.31
CN 103366278 A,2013.10.23
CN 104270752 A,2015.01.07
CN 104869570 A,2015.08.26
CN 106357393 A,2017.01.25
CN 106571907 A,2017.04.19
CN 1806410 A,2006.07.19
EP 2950195 A1,2015.12.02
汤迪斌."一种TCP连接的延迟多次迁移技术".《计算机工程应用》.2008,全文.

审查员 张琳

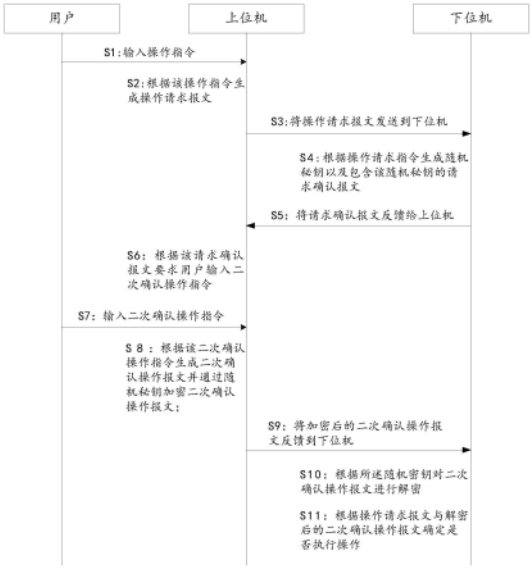
权利要求书2页 说明书6页 附图2页

(54)发明名称

# 单通道实现请求确认操作的方法及系统

(57)摘要

本发明的目的在于解决现有技术所存在的问题,找到一种单通道实现请求确认操作的方法及系统,提高安全性。包括下位机接收上位机发送的操作请求报文,根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文,将请求确认报文反馈给上位机;上位机接收到请求确认报文时,接收用户输入的二次确认操作指令,根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文,将加密后的二次确认操作报文反馈到下位机;下位机根据随机密钥对二次确认操作报文进行解密,根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。有益技术效果:单通道实现请求确认操作,防止因为旧指令的重发而引发安全事故。




CN 107959552 B

1.单通道实现请求确认操作的方法,其特征在于,包括:

通过上位机接收用户输入的操作指令,根据该操作指令生成操作请求报文,将操作请求报文发送到下位机;等待下位机反馈的请求确认报文,当接收到请求确认报文时,根据该请求确认报文要求用户输入二次确认操作指令;接收用户输入的二次确认操作指令,根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文,将加密后的二次确认操作报文反馈到下位机;

通过下位机接收上位机发送的操作请求报文,根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文,将请求确认报文反馈给上位机;等待上位机反馈的二次确认操作报文,当接收到二次确认操作报文时,根据所述随机秘钥对二次确认操作报文进行解密,根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

2.如权利要求1所述的单通道实现请求确认操作的方法,其特征在于,所述操作请求报文包含有操作指令的数据校验码;所述下位机接收上位机发送的操作请求报文时,根据数据校验码验证操作请求报文,如果验证不通过,则终止操作指令。

3.如权利要求1或2所述的单通道实现请求确认操作的方法,其特征在于,下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时,在请求确认报文中增加随机验证题目;

上位机接收到请求确认报文时,根据该请求确认报文要求用户输入随机验证题目答案,并在二次确认操作报文中增加所述随机验证题目答案;

所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括:如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致,则执行操作;否则不执行操作。

4.如权利要求1所述的单通道实现请求确认操作的方法,其特征在于,上位机等待下位机反馈的请求确认报文时,如果预设时间内未收到接收请求确认报文,则终止操作指令;和/或,等待上位机反馈的二次确认操作报文时,如果设定时间内未接收到二次确认操作报文,则终止操作指令。

5.如权利要求1所述的单通道实现请求确认操作的方法,其特征在于,所述二次确认操作指令的格式与所述操作指令的格式不同。

6.单通道实现请求确认操作的系统,其特征在于,包括上位机和下位机,其中,

上位机接收用户输入的操作指令,根据该操作指令生成操作请求报文,将操作请求报文发送到下位机;等待下位机反馈的请求确认报文,当接收到请求确认报文时,根据该请求确认报文要求用户输入二次确认操作指令;接收用户输入的二次确认操作指令,根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文,将加密后的二次确认操作报文反馈到下位机;

下位机接收上位机发送的操作请求报文,根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文,将请求确认报文反馈给上位机;等待上位机反馈的二次确认操作报文,当接收到二次确认操作报文时,根据所述随机秘钥对二次确认操作报文进行解密,根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

7.如权利要求6所述的单通道实现请求确认操作的系统,其特征在于,所述操作请求报文包含有操作指令的数据校验码;所述下位机接收上位机发送的操作请求报文时,根据数

据校验码验证操作请求报文，如果验证不通过，则终止操作指令。

8.如权利要求6或7所述的单通道实现请求确认操作的系统，其特征在于，下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时，在请求确认报文中增加随机验证题目；

上位机接收到请求确认报文时，根据该请求确认报文要求用户输入随机验证题目答案，并在二次确认操作报文中增加所述随机验证题目答案；

所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括：如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致，则执行操作；否则不执行操作。

9.如权利要求6所述的单通道实现请求确认操作的系统，其特征在于，上位机等待下位机反馈的请求确认报文时，如果预设时间内未收到接收请求确认报文，则终止操作指令；

和/或，等待上位机反馈的二次确认操作报文时，如果设定时间内未接收到二次确认操作报文，则终止操作指令。

10.如权利要求6所述的单通道实现请求确认操作的系统，其特征在于，所述二次确认操作指令的格式与所述操作指令的格式不同。

# 单通道实现请求确认操作的方法及系统

## 技术领域

[0001] 本发明涉及轨道安全通信领域，具体涉及一种单通道实现请求确认操作的方法及系统。

## 背景技术

[0002] 现有技术中上位机(非安全)的操作指令和确认指令通过安全协议向下位机(安全)下发；即上位机发送操作指令和确认指令，下位机根据操作指令和确认指令判断是否执行操作指令，由于上位机是不安全的，可能重复发送操作指令和确认指令，进而出现误操作的情况，存在安全隐患。

## 发明内容

[0003] 本发明的目的在于解决现有技术所存在的问题，找到一种单通道实现请求确认操作的方法及系统，提高安全性。

[0004] 为了实现所述目的，本发明单通道实现请求确认操作的方法，包括：

[0005] 通过上位机接收用户输入的操作指令，根据该操作指令生成操作请求报文，将操作请求报文发送到下位机；等待下位机反馈的请求确认报文，当接收到请求确认报文时，根据该请求确认报文要求用户输入二次确认操作指令；接收用户输入的二次确认操作指令，根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文，将加密后的二次确认操作报文反馈到下位机；

[0006] 通过下位机接收上位机发送的操作请求报文，根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文，将请求确认报文反馈给上位机；等待上位机反馈的二次确认操作报文，当接收到二次确认操作报文时，根据所述随机密钥对二次确认操作报文进行解密，根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

[0007] 优选的，所述操作请求报文包含有操作指令的数据校验码；所述下位机接收上位机发送的操作请求报文时，根据数据校验码验证操作请求报文，如果验证不通过，则终止操作指令。

[0008] 优选的，下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时，在请求确认报文中增加随机验证题目；上位机接收到请求确认报文时，根据该请求确认报文要求用户输入随机验证题目答案，并在二次确认操作报文中增加所述随机验证题目答案；所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括：如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致，则执行操作；否则不执行操作。

[0009] 优选的，上位机等待下位机反馈的请求确认报文时，如果预设时间内未收到接收请求确认报文，则终止操作指令；和/或，等待上位机反馈的二次确认操作报文时，如果设定时间内未接收到二次确认操作报文，则终止操作指令。

[0010] 优选的，所述二次确认操作指令的格式与所述操作指令的格式不同。

[0011] 作为本发明的另一方面，本发明单通道实现请求确认操作的系统，包括上位机和下位机，其中，

[0012] 上位机接收用户输入的操作指令，根据该操作指令生成操作请求报文，将操作请求报文发送到下位机；等待下位机反馈的请求确认报文，当接收到请求确认报文时，根据该请求确认报文要求用户输入二次确认操作指令；接收用户输入的二次确认操作指令，根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文，将加密后的二次确认操作报文反馈到下位机；

[0013] 下位机接收上位机发送的操作请求报文，根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文，将请求确认报文反馈给上位机；等待上位机反馈的二次确认操作报文，当接收到二次确认操作报文时，根据所述随机密钥对二次确认操作报文进行解密，根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

[0014] 优选的，所述操作请求报文包含有操作指令的数据校验码；所述下位机接收上位机发送的操作请求报文时，根据数据校验码验证操作请求报文，如果验证不通过，则终止操作指令。

[0015] 优选的，下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时，在请求确认报文中增加随机验证题目；上位机接收到请求确认报文时，根据该请求确认报文要求用户输入随机验证题目答案，并在二次确认操作报文中增加所述随机验证题目答案；所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括：如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致，则执行操作；否则不执行操作。

[0016] 优选的，上位机等待下位机反馈的请求确认报文时，如果预设时间内未收到接收请求确认报文，则终止操作指令；和/或，等待上位机反馈的二次确认操作报文时，如果设定时间内未接收到二次确认操作报文，则终止操作指令。

[0017] 优选的，所述二次确认操作指令的格式与所述操作指令的格式不同。

[0018] 通过实施本发明可以取得以下有益技术效果：由于二次确认操作报文通过下位机生成的随机秘钥加密，而随机秘钥是下位机在接收上位机操作请求报文时生成的动态密码，所以上位机发送的旧指令采用的随机秘钥与本次新指令采用的随机秘钥不同，进而防止因为旧指令的重发而引发安全事故。

## 附图说明

[0019] 图1为本发明实施例1中的方法流程图；

[0020] 图2为本发明实施例2中的方法流程图；

## 具体实施方式

[0021] 为了便于本领域技术人员的理解，下面结合具体实施例对本发明作进一步的说明：

[0022] 实施例1：

[0023] 本发明单通道实现请求确认操作的方法，包括：

[0024] 通过上位机接收用户输入的操作指令，根据该操作指令生成操作请求报文，将操

作请求报文发送到下位机;等待下位机反馈的请求确认报文,当接收到请求确认报文时,根据该请求确认报文要求用户输入二次确认操作指令;接收用户输入的二次确认操作指令,根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文,将加密后的二次确认操作报文反馈到下位机;

[0025] 通过下位机接收上位机发送的操作请求报文,根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文,将请求确认报文反馈给上位机;等待上位机反馈的二次确认操作报文,当接收到二次确认操作报文时,根据所述随机密钥对二次确认操作报文进行解密,根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

[0026] 通过实施本发明可以取得以下有益技术效果:下位机在接收到上位机的操作请求报文时反馈包含随机秘钥的请求确认报文用以触发上位机生成二次确认操作报文;上位机通过获取用户输入的二次确认操作指令生成通过随机秘钥加密的二次确认操作报文,并将二次确认操作报文发送到下位机;下位机通过随机秘钥解密二次确认操作报文,并根据操作请求报文与二次确认操作报文判断操作指令与二次确认操作指令是否一致,进而确定是否执行操作指令。由于二次确认操作报文通过下位机生成的随机秘钥加密,而随机秘钥是下位机在接收上位机操作请求报文时生成的动态密码,所以上位机发送的旧指令采用的随机秘钥与本次新指令采用的随机秘钥不同,进而防止因为旧指令的重发而引发安全事故。

[0027] 为了便于理解,如图1所示,作为本实施例的一种实施方式,其步骤如下:

[0028] S1:用户输入操作指令;

[0029] S2:上位机接收用户输入的操作指令;根据该操作指令生成操作请求报文;

[0030] S3:上位机将操作请求报文发送到下位机;

[0031] S4:下位机接收上位机发送的操作请求报文;根据操作请求指令生成随机秘钥以及包含该随机秘钥的请求确认报文;

[0032] S5:上位机将请求确认报文反馈给上位机;

[0033] S6:上位机接收上位机反馈的请求确认报文,根据该请求确认报文要求用户输入二次确认操作指令;

[0034] S7:用户输入二次确认操作指令;

[0035] S8:上位机接收用户输入的二次确认操作指令;根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文;

[0036] S9:将加密后的二次确认操作报文反馈到下位机;

[0037] S10:下位机根据所述随机密钥对二次确认操作报文进行解密;

[0038] S11:下位机根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

[0039] 其中,步骤S11中,所述下位机根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令可以为:操作请求报文中的操作指令与二次确认操作报文中的操作指令一致,则执行操作,否则不执行操作。其中,作为一种优选,不执行操作时,可以提醒用户。

[0040] 作为上述单通道实现请求确认操作的方法的优选实施方式,所述操作请求报文包含有操作指令的数据校验码;所述下位机接收上位机发送的操作请求报文时,根据数据校验码验证操作请求报文,如果验证不通过,则终止操作指令。通过数据校验码校验,可以排除通信错误,提高安全性。

[0041] 作为上述单通道实现请求确认操作的方法的优选实施方式，上位机等待下位机反馈的请求确认报文时，如果预设时间内未收到接收请求确认报文，则终止操作指令；预设时间内未收到接收请求确认报文，即发生了异常情况，通过终止操作指令的方式防止发生安全事故，提高安全性。预设时间可以根据实际设置，如设置成30秒等。

[0042] 作为上述单通道实现请求确认操作的方法的优选实施方式，等待上位机反馈的二次确认操作报文时，如果设定时间内未接收到二次确认操作报文，则终止操作指令。设定时间内未接收到二次确认操作报文，即发生了异常情况，通过终止操作指令的方式防止发生安全事故，提高安全性。设定时间可以根据实际设置，如设置成30秒等。

[0043] 作为上述单通道实现请求确认操作的方法的优选实施方式，所述二次确认操作指令的格式与所述操作指令的格式不同。由于两次指令要求的输入格式不一样，能识别上位机的共因故障导致的数据被修改的风险，也可以排除通信错误导致的问题，进而提高提高安全性。

[0044] 为了提高安全性，本发明中还可以在各报文中增加序列号、处理号字段，时间信息，防止重复、删除、乱序；

[0045] 实施例2：

[0046] 与实施例1的区别在于：下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时，在请求确认报文中增加随机验证题目；上位机接收到请求确认报文时，根据该请求确认报文要求用户输入随机验证题目答案，并在二次确认操作报文中增加所述随机验证题目答案；所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括：如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致，则执行操作；否则不执行操作。

[0047] 通过确认验证题目答案，可以排除非用户输入情况下，上位机自己异常产生指令的情况。

[0048] 为了便于理解，如图2所示，作为本实施例的一种实施方式，其步骤如下：

[0049] Y1：用户输入操作指令；

[0050] Y2：上位机接收用户输入的操作指令；根据该操作指令生成操作请求报文；

[0051] Y3：上位机将操作请求报文发送到下位机；

[0052] Y4：下位机接收上位机发送的操作请求报文；根据操作请求指令生成随机秘钥以及包含该随机秘钥的请求确认报文；在请求确认报文中增加随机验证题目；

[0053] Y5：上位机将请求确认报文反馈给上位机；

[0054] Y6：上位机接收上位机反馈的请求确认报文，根据该请求确认报文要求用户输入二次确认操作指令和随机验证题目答案；

[0055] Y7：用户输入二次确认操作指令和随机验证题目答案；

[0056] Y8：上位机接收用户输入的二次确认操作指令和随机验证题目答案；根据该二次确认操作指令生成二次确认操作报文，并在二次确认操作报文中增加随机验证题目答案，通过随机秘钥加密二次确认操作报文；

[0057] Y9：将加密后的二次确认操作报文反馈到下位机；

[0058] Y10：下位机根据所述随机密钥对二次确认操作报文进行解密；

[0059] Y11：下位机根据操作请求报文与解密后的二次确认操作报文确定是否执行操作

指令。

[0060] 实施例3：

[0061] 作为本发明的另一方面，本发明单通道实现请求确认操作的系统。

[0062] 包括上位机和下位机，

[0063] 其中，上位机接收用户输入的操作指令，根据该操作指令生成操作请求报文，将操作请求报文发送到下位机；等待下位机反馈的请求确认报文，当接收到请求确认报文时，根据该请求确认报文要求用户输入二次确认操作指令；接收用户输入的二次确认操作指令，根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文，将加密后的二次确认操作报文反馈到下位机；

[0064] 下位机接收上位机发送的操作请求报文，根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文，将请求确认报文反馈给上位机；等待上位机反馈的二次确认操作报文，当接收到二次确认操作报文时，根据所述随机密钥对二次确认操作报文进行解密，根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令。

[0065] 通过实施本发明可以取得以下有益技术效果：下位机在接收到上位机的操作请求报文时反馈包含随机秘钥的请求确认报文用以触发上位机生成二次确认操作报文；上位机通过获取用户输入的二次确认操作指令生成通过随机秘钥加密的二次确认操作报文，并将二次确认操作报文发送到下位机；下位机通过随机秘钥解密二次确认操作报文，并根据操作请求报文与二次确认操作报文判断操作指令与二次确认操作指令是否一致，进而确定是否执行操作指令。由于二次确认操作报文通过下位机生成的随机秘钥加密，而随机秘钥是下位机在接收上位机操作请求报文时生成的动态密码，所以上位机发送的旧指令采用的随机秘钥与本次新指令采用的随机秘钥不同，进而防止因为旧指令的重发而引发安全事故。

[0066] 作为上述单通道实现请求确认操作的系统的优选实施方式，所述操作请求报文包含有操作指令的数据校验码；所述下位机接收上位机发送的操作请求报文时，根据数据校验码验证操作请求报文，如果验证不通过，则终止操作指令。

[0067] 作为上述单通道实现请求确认操作的系统的优选实施方式，下位机根据操作请求报文生成随机秘钥以及包含该随机秘钥的请求确认报文时，在请求确认报文中增加随机验证题目；上位机接收到请求确认报文时，根据该请求确认报文要求用户输入随机验证题目答案，并在二次确认操作报文中增加所述随机验证题目答案；所述根据操作请求报文与解密后的二次确认操作报文确定是否执行操作指令包括：如果随机验证题目答案正确且操作请求报文中的操作指令与二次确认操作报文中的操作指令一致，则执行操作；否则不执行操作。

[0068] 作为上述单通道实现请求确认操作的系统的优选实施方式，上位机等待下位机反馈的请求确认报文时，如果预设时间内未收到接收请求确认报文，则终止操作指令；和/或，等待上位机反馈的二次确认操作报文时，如果设定时间内未接收到二次确认操作报文，则终止操作指令。

[0069] 作为上述单通道实现请求确认操作的系统的优选实施方式，所述二次确认操作指令的格式与所述操作指令的格式不同。

[0070] 由于本实施例中的系统与实施例1和实施例2中的方法相对应，故相关内容本实施例不再重复描述。

[0071] 以上所述仅为本发明的具体实施例,但本发明的技术特征并不局限于此,任何本领域的技术人员在本发明的领域内,所作的变化或修饰皆涵盖在本发明的专利范围之中。

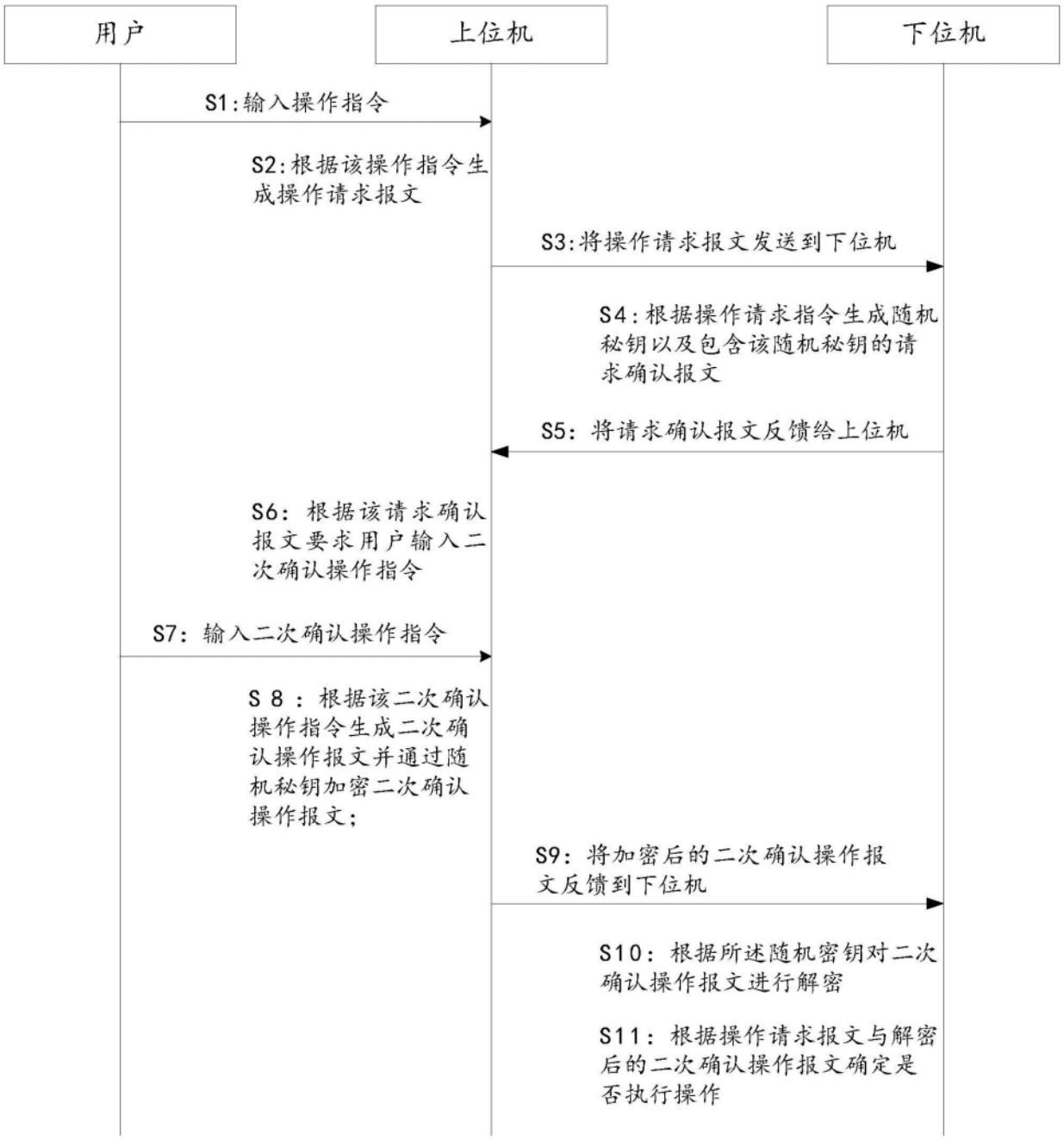

用户
上位机
下位机
S1:输入操作指令
S2:根据该操作指令生成操作请求报文
S3:将操作请求报文发送到下位机
S4:根据操作请求指令生成随机秘钥以及包含该随机秘钥的请求确认报文
S5:将请求确认报文反馈给上位机
S6:根据该请求确认报文要求用户输入二次确认操作指令
S7:输入二次确认操作指令
S8:根据该二次确认操作指令生成二次确认操作报文并通过随机秘钥加密二次确认操作报文;
S9:将加密后的二次确认操作报文反馈到下位机
S10:根据所述随机密钥对二次确认操作报文进行解密
S11:根据操作请求报文与解密后的二次确认操作报文确定是否执行操作

图1

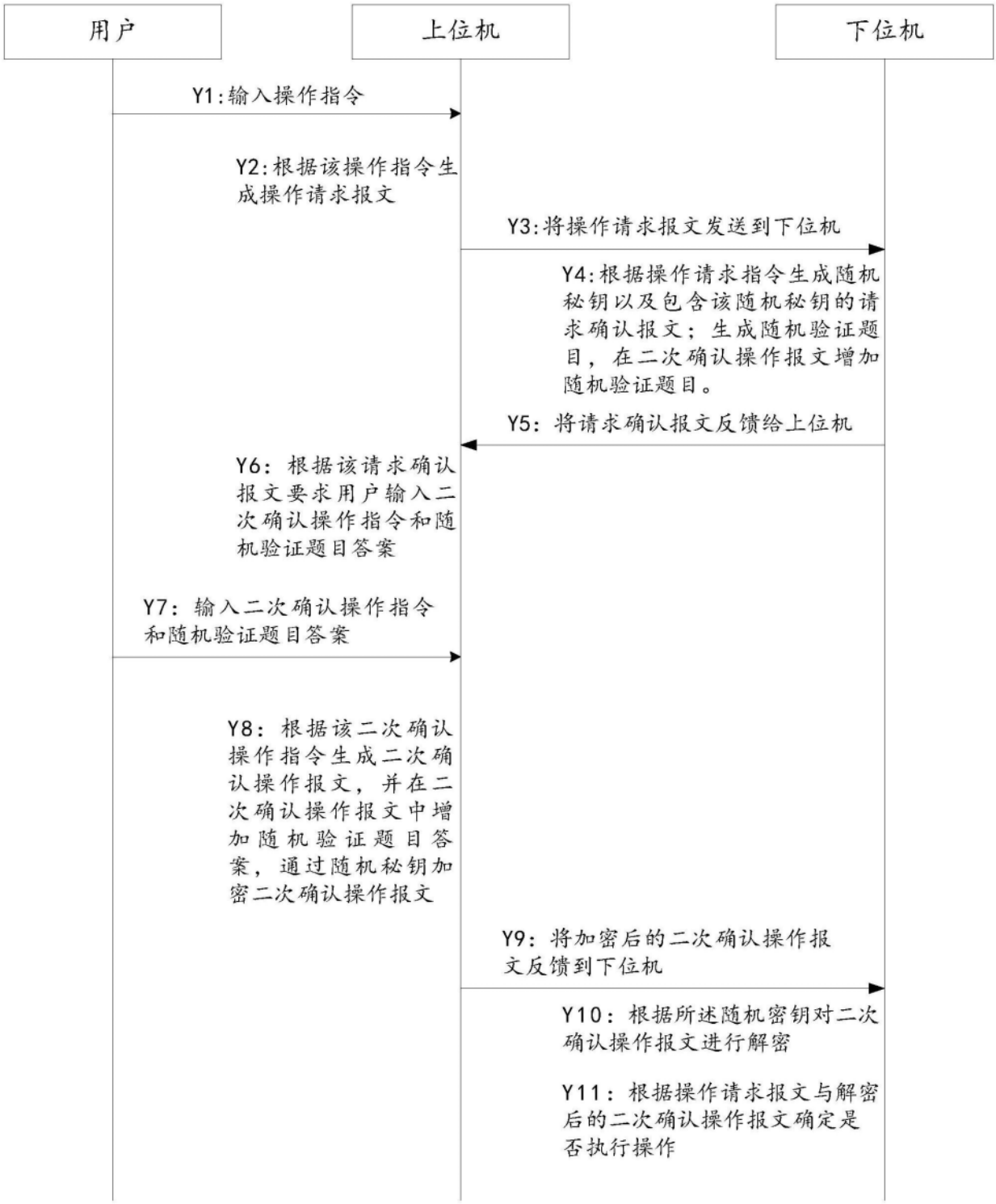

用户
上位机
下位机
Y1:输入操作指令
Y2:根据该操作指令生成操作请求报文
Y3:将操作请求报文发送到下位机
Y4:根据操作请求指令生成随机秘钥以及包含该随机秘钥的请求确认报文；生成随机验证题目，在二次确认操作报文增加随机验证题目。
Y5：将请求确认报文反馈给上位机
Y6：根据该请求确认报文要求用户输入二次确认操作指令和随机验证题目答案
Y7：输入二次确认操作指令和随机验证题目答案
Y8：根据该二次确认操作指令生成二次确认操作报文，并在二次确认操作报文中增加随机验证题目答案，通过随机秘钥加密二次确认操作报文
Y9：将加密后的二次确认操作报文反馈到下位机
Y10：根据所述随机密钥对二次确认操作报文进行解密
Y11：根据操作请求报文与解密后的二次确认操作报文确定是否执行操作

图2